REMARKS

Claims 1 and 2 are amended hereby. Claim 8 is added. No claims are canceled. Accordingly, after entry of this amendment, claims 1-8 will remain pending and under consideration.

In the Office Action, the Examiner objected to claim 2, stating that the claim contained an informality. In particular, the Examiner found a typographical error in the phrase "using a first a second subkeys respectively." The Examiner suggested correcting the phrase to read "using a first subkey and a second subkey." In response, the Applicant has amended the claim in the manner suggested by the Examiner.

The Examiner rejected claim 1 under 35 U.S.C. § 103(a) as being unpatentable over Luyster (U.S. Patent No. 6,578,150) in view of Baji et al. (U.S. Patent No. 4,825,287). The Applicant respectfully disagrees with this rejection and, therefore, respectfully traverses the rejection.

The Examiner objected to claims 2-6, stating that claims 2-6 depended from a rejected base claim. The Examiner also stated that claims 2-6 would be considered allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The Applicant would like to thank the Examiner for the indication of allowable subject matter.

The Applicant respectfully points out that the amendments presented by this Amendment are intended to broaden the scope of the claims. The Applicant respectfully submits that, as would be appreciated by those skilled in the art, the present invention is not solely applicable to a 64-bit block cipher. Instead, the present invention may be applied to block ciphering with various bit sizes. While the claims are broader in scope as a result of the amendments presented herein, the Applicant respectfully submits that the

claims, as now presented, are patentable over the prior art relied upon by the Examiner.

Claims 1-8 recite an apparatus for encrypting N-bit plain text blocks that combines a number of features including, among them, an input means responsive to a first clock, an output means responsive to a second clock, and an encryption means using the first and second clocks. In two contemplated embodiments, the input means 610 and 620 and the output means 640 and 650 respond to the first and second clocks, respectively. (See, e.g., Fig. 6.) The encryption means operates in response to both the first and second clocks. (See, e.g., Fig. 6, and the specification at page 12, line 14, through page 13, line 17.) Among other features, this combination is not disclosed or suggested by the references relied upon by the Examiner to reject claim 1.

As recognized by the Examiner at paragraph 5 of the Office Action, Luyster, among other things, fails to describe an apparatus where the input means 52 and 54 and the output means 84 and 86 are controlled by first and second clocks. Contrary to the Examiner's assertion, the Applicant respectfully submits that Baji et al. fails to correct this deficiency. Referring to Figs. 6 and 7 of Baji et al., the Applicant respectfully emphasizes that the second internal clock ϕ_2 does not assist in generating the 3-bit program memory addreses a0, a1, and a2. From the figures, it appears that clock ϕ_1 is solely responsible for this function. The Applicant respectfully submits that the specification of Baji et al. appears to support this conclusion. For example, Baji et al. states that:

> Master/slave latches are used here so that the data is latched in response to the first phase clock ϕ_1 and appear in response to a second phase clock ϕ_2. As a result, the data is fed to the multiplier 5 at the instant when the clock ϕ_2 rises at the latter half of the first program step.

(Baji et al. at col. 5, lines 10-15.) In addition, Baji et al. relays:

> A voltage controlled oscillator 19 generates two-phase clocks

> ϕ_1 and ϕ_2, which are counted down by a binary counter 20 which is reset every 5 counts in accordance with the fifth program step. Here, 3-bit program memory addresses (a0, a1 and a2) are generated. An accurate synchronization is taken by comparing the phases of the counted-down result a_2 and the sampling clock CLKS of the input signal by means of a phase comparator 17.

(Baji et al., at col. 6, lines 56-64.) In other words, at a minimum, Baji et al. appears to rely upon a single clock with two phases, ϕ_1 and ϕ_2, not two separate clocks.

Accordingly, the Applicant respectfully submits that neither reference, either alone or in combination describes or suggests the features as combined in claims 1-8. As a result, the Applicant respectfully submits that claims 1-8 are patentable thereover.

In view of the above amendments and remarks, Applicant respectfully submits that all of the claims are allowable and that the entire application is in condition for allowance.

Should the Examiner believe that anything further is desirable to place the application in better condition for allowance, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Please charge any fees associated with the submission of this paper to Deposit Account Number 033975. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced Deposit Account.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

JEFFREY D. KARCESKI
Reg. No. 35914
Tel. No. 703 905.2110
Fax No. 703.905.2500

Date: June 14, 2005
P.O. Box 10500
McLean, VA 22102
(703) 905-2000